1/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:DERWENT WPI

011885385 **Image available**
WPI Acc No: 1998-302295/**199827**
XRPX Acc No: N98-236871
Network authentication system for multiple services - notifies address of particular service to partition system after checking received user ID and password with reference to table
Patent Assignee: FUJITSU LTD (FUIT)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 10105516	A	19980424	JP 97116899	A	19970507	199827	B

Priority Applications (No Type Date): JP 96122914 A 19960517
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 10105516	A		8	G06F-015/00	

Abstract (Basic): JP 10105516 A
The system detects calling to the access point of the network. Then, the user ID and password are forwarded to a network authentication mechanism (6).
The mechanism checks the user ID and password with reference to a table and notifies an address of a particular service to a partition system (4). The partition system is connected to several services.
ADVANTAGE - Raises reliability of network security. Reduces burden of security management.
Dwg.1/5
Title Terms: NETWORK; AUTHENTICITY; SYSTEM; MULTIPLE; SERVICE; NOTIFICATION ; ADDRESS; SERVICE; PARTITION; SYSTEM; AFTER; CHECK; RECEIVE; USER; ID; PASSWORD; REFERENCE; TABLE
Derwent Class: T01; W01
International Patent Class (Main): G06F-015/00
International Patent Class (Additional): G06F-001/00; G06F-013/00; H04L-012/22; H04M-003/42; H04M-011/00
File Segment: EPI

1/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

05822416 **Image available**
NETWORK AUTHENTICATION SYSTEM

PUB. NO.: 10-105516 A]
PUBLISHED: April 24, 1998 (19980424)
INVENTOR(s): SAWA HIROSHI
APPLICANT(s): FUJITSU LTD [000522] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 09-116899 [JP 97116899]
FILED: May 07, 1997 (19970507)
INTL CLASS: [6] G06F-015/00; G06F-001/00; G06F-013/00; H04L-012/22; H04M-003/42; H04M-011/00
JAPIO CLASS: 45.4 (INFORMATION PROCESSING -- Computer Applications); 36.4 (LABOR SAVING DEVICES -- Service Automation); 44.3 (COMMUNICATION -- Telegraphy); 44.4 (COMMUNICATION -- Telephone); 45.2 (INFORMATION PROCESSING -- Memory Units); 45.9 (INFORMATION PROCESSING -- Other)

ABSTRACT

PROBLEM TO BE SOLVED: To improve the reliability of network security and to improve the security management of a service provider or to reduce the burden of security management by performing the security management at the entrance of a network by performing user authentication on the network when providing plural services from the same public access point, and connecting the access point while distributing it to the relevant service.

SOLUTION: A distributing mechanism 4 detects an incoming call from a user terminal 1 through a public line 2 to the access point of a certain network, transfers a user ID and a password to a network authentication mechanism 6 and connected any service designated out of plural services. While referring to a table 9 based on the user ID and the password transferred from this distributing mechanism 4, the relevant user ID and password are checked and in case of OK, the address of the relevant service is reported to the distributing mechanism 4.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－105516

(43)公開日　平成10年(1998)４月24日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｂ
	1/00	３７０		1/00	３７０Ｅ
	13/00	３５１		13/00	３５１Ａ
Ｈ０４Ｌ	12/22		Ｈ０４Ｍ	3/42	Ｚ
Ｈ０４Ｍ	3/42			11/00	３０２

審査請求　未請求　請求項の数４　ＯＬ　（全８頁）　最終頁に続く

(21)出願番号　特願平9－116899

(22)出願日　平成９年(1997)５月７日

(31)優先権主張番号　特願平8－122914

(32)優先日　平８(1996)５月17日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　梅　博史
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

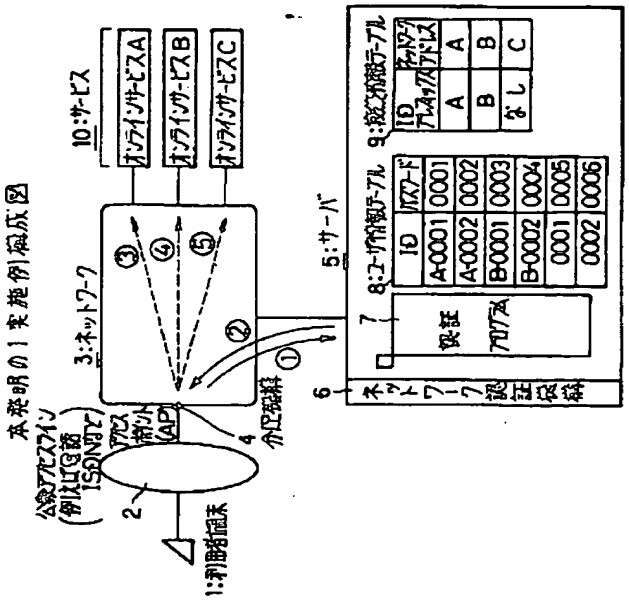
(74)代理人　弁理士　岡田　守弘

(54)【発明の名称】　ネットワーク認証システム

(57)【要約】

【課題】　本発明は、ネットワーク認証システムに関し、同一公衆アクセスポイントから複数のサービスを提供する際に、ネットワークでのユーザ認証を行なうと共に該当するサービスに分配して接続し、ネットワークの入口でセキュリティ管理を行い、ネットワークセキュリティの信頼性を高めると共にサービス提供者のセキュリティ管理を高めたり、セキュリティ管理の負担を軽減したりすることを目的とする。

【解決手段】　利用者端末から公衆回線を介してあるネットワークのアクセスポイントへの着呼を検出して利用者ＩＤおよびパスワードをネットワーク認証機構に転送し、複数のサービスのうちの指定されたサービスに接続する分配機構と、この分配機構から転送されてきた利用者ＩＤおよびパスワードをもとに、テーブルを参照して当該利用者ＩＤおよびパスワードをチェックしてＯＫのときに該当サービスのアドレスを分配機構に通知するネットワーク認証機構とを備えるように構成する。



1

【特許請求の範囲】

【請求項１】複数のサービスの認証を行なうネットワーク認証システムにおいて、

利用者端末から公衆回線を介してあるネットワークのアクセスポイントへの着呼を検出して利用者ＩＤおよびパスワードをネットワーク認証機構に転送し、複数のサービスのうちの指定されたサービスに接続する分配機構と、

この分配機構から転送されてきた利用者ＩＤおよびパスワードをもとに、テーブルを参照して当該利用者ＩＤおよびパスワードをチェックしてＯＫのときに該当サービスのアドレスを上記分配機構に通知するネットワーク認証機構とを備えたことを特徴とするネットワーク認証システム。

【請求項２】複数のサービスの認証を行なうネットワーク認証システムにおいて、

利用者端末から公衆回線を介してあるネットワークのアクセスポイントへの着呼を検出して利用者ＩＤおよびパスワードを認証サーバ中継機構に転送し、複数のサービスのうちの指定されたサービスに接続する分配機構と、上記分配機構から転送されてきた利用者ＩＤおよびパスワードについて、テーブルを参照して当該利用者ＩＤのサービスの認証を担当するサーバに転送してチェックさせ、ＯＫの返答のあったアドレスを上記分配機構に通知する認証サーバ中継機構と、

上記認証サーバ中継機構から転送されてきた利用者ＩＤおよびパスワードをもとに、テーブルを参照して当該利用者ＩＤおよびパスワードをチェックしてＯＫのときに該当サービスのアドレスを上記認証サーバ中継機構に通知するサーバとを備えたことを特徴とするネットワーク認証システム。

【請求項３】上記利用者ＩＤの一部を上記サービスに対応づけたことを特徴とする請求項１あるいは請求項２記載のネットワーク認証システム。

【請求項４】利用者端末から公衆回線を介してあるネットワークのアクセスポイントへの着呼を検出して利用者ＩＤおよびパスワードをネットワーク認証機構に転送し、複数のサービスのうちの指定されたサービスに接続する分配機構と、

この分配機構から転送されてきた利用者ＩＤおよびパスワードをもとに、テーブルを参照して当該利用者ＩＤおよびパスワードをチェックしてＯＫのときに該当サービスのアドレスを上記分配機構に通知するネットワーク認証機構とを機能させるプログラムを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数のサービスの認証を行なうネットワーク認証システムに関するものである。

【０００２】

2

【従来の技術】従来、公衆回線を介してネットワークに接続してサービスを提供する場合、サービス毎に専用のアクセスポイント（例えば専用の電話番号）を設け、当該アクセスポイントからネットワークを介して該当オンラインサービスに接続し、当該オンラインサービスで認証（ユーザＩＤおよびパスワードの認証）を行なう。

【０００３】また、商用オンラインサービス事業者が、同一公衆アクセスポイントから複数のサービスを提供する場合、図４に示すように、単にオンラインサービス毎に分配して接続し、接続先のオンラインサービスの入口で認証をそれぞれ個別に行なうようにしていた。

【０００４】また、商用オンラインサービス事業者が、同一公衆アクセスポイントから複数のサービスを提供する場合、図５に示すように、あるオンラインサービスで認証を行い、ゲートウェイ機能によって他のオンラインサービスに接続するようにしていた。

【０００５】以下図４および図５の構成および動作を簡単に説明する。図４は、従来技術の説明図（その１）を示す。図４において、公衆アクセスラインは、利用者端末からオンラインサービスの提供を受けるためのアクセスポイントＡＰに接続するための公衆網である。

【０００６】ネットワークは、オンラインサービスの提供を行なう事業者のネットワークである。オンラインサービスＡ、Ｂは、複数の種類のサービス、例えばパソコン通信、インターネット接続サービスなどのオンラインサービスを提供するサーバなどであって、オンラインサービス機能、およびユーザ認証機能などから構成されるものである。

【０００７】オンラインサービス機能は、オンラインで各種サービスを利用者に提供するものである。ユーザ認証機能は、ユーザのユーザＩＤおよびパスワードの認証を行なうものである。

【０００８】次に、動作を説明する。

利用者端末からアクセスポイントに電話する。

で電話を受信したネットワークが利用者端末からの指定をもとに該当するオンラインサービスＡあるいはオンラインサービスＢに接続する。

【０００９】　　で接続されたオンラインサービスＡあるいはオンラインサービスＢがユーザＩＤおよびパスワードの認証を行い、ＯＫのときにサービスの提供をそれぞれ行なう。

【００１０】図５は、従来技術の説明図（その２）を示す。図５において、公衆アクセスラインは、利用者端末からオンラインサービスの提供を受けるためのアクセスポイントＡＰに接続するための公衆網である。

【００１１】ネットワークは、オンラインサービスの提供を行なう事業者のネットワークである。オンラインサービスＡは、オンラインサービスを提供するサーバなどであって、ここでは、ゲートウェイ機能、オンラインサービス機能、およびユーザ認証機能などから構成される

ものである。

【００１２】ゲートウェイ機能は、該当する他のオンラインサービスに転送するものである。オンラインサービス機能は、オンラインで各種サービスを利用者に提供するものである。

【００１３】ユーザ認証機能は、ユーザのユーザＩＤおよびパスワードの認証を行なうものである。次に、動作を説明する。

【００１４】　利用者端末からアクセスポイントに電話する。

　で電話を受信したネットワークがここでは固定的な１つのオンラインサービスＡに接続する。

【００１５】　で接続されたオンラインサービスＡがユーザＩＤおよびパスワードの認証を行い、ＯＫのときにサービスを提供、あるいはゲートウェイ機能が更に他のオンラインサービスに接続する。

【００１６】　でゲートウェイ機能によって接続された他のオンラインサービス、例えばオンラインサービスＢがサービスを提供、あるいは更にユーザＩＤおよびパスワードの認証を行い、ＯＫのときにサービスの提供を行なう。

【００１７】

【発明が解決しようとする課題】上述したように、従来の図４の構成のもとでは、（１）　異なるオンラインサービスで、アクセスポイントを共用できるが、（２）　ネットワーク側でのユーザ認証ができなく（３）　オンラインサービスを提供する側でユーザ認証（ユーザＩＤおよびパスワードによる認証）を行なうため、ネットワークの入口で認証を行なうことができなくセキュリティに欠けると共に、新たなサービスを提供するオンラインサービスでは全ての認証を行ってセキュリティを確保する必要が生じてしまうという問題があった。

【００１８】また、上述したように、従来の図５の構成のもとでは、（１）　異なるオンラインサービスで、アクセスポイントを共用できるが、（２）　ネットワーク側でのユーザ認証がなく（３）　オンラインサービスを提供する側でユーザ認証（ユーザＩＤおよびパスワードによる認証）を行なう（４）　ゲートウェイ機能を持たないオンラインサービスは、ゲートウェイ機能を有するオンラインサービスのユーザからしかサービス提供を受けることができないため、ネットワークの入口で認証を行なうことができなくセキュリティに欠けると共に、新たなサービスを提供するオンラインサービスでは全ての認証を行ってセキュリティを確保する必要が生じてしまい、更にゲートウェイ機能の有無によって受けられるサービスに制限を生じてしまうという問題があった。

【００１９】本発明は、これらの問題を解決するため、同一公衆アクセスポイントから複数のサービスを提供する際に、ネットワークでのユーザ認証を行なうと共に該当するサービスに分配して接続し、ネットワークの入口でセキュリティ管理を行い、ネットワークセキュリティの信頼性を高めると共にサービス提供者のセキュリティ管理を高めたり、セキュリティ管理の負担を軽減したりすることを目的としている。

【００２０】

【課題を解決するための手段】図１および図２を参照して課題を解決するための手段を説明する。図１および図２において、利用者端末１は、利用者ＩＤおよびパスワードを入力してサービスを利用するものである。

【００２１】分配機構４は、利用者端末１からの着呼を検出して利用者ＩＤおよびパスワードをネットワーク認証機構６や認証サーバ中継機構１２に転送したり、複数のサービスのうちの指定されたサービス１０に接続したりなどするものである。

【００２２】サービス１０は、各種サービスを提供するものである。次に、動作を説明する。ネットワーク３の分配機構４が利用者端末１から公衆回線を介してアクセスポイントへの着呼を検出し、利用者ＩＤおよびパスワードをネットワーク認証機構６に転送し、ネットワーク認証機構６が利用者ＩＤおよびパスワードをもとにテーブルを参照しチェックしてＯＫのときにサービスのアドレスを分配機構４に通知し、分配機構４が指定されたアドレスに接続し、利用者端末１と該当するサービス１０を接続し、当該利用者端末１がサービス１０からサービス提供を受けるようにしている。

【００２３】また、ネットワーク３の分配機構４が利用者端末１から公衆回線を介してアクセスポイントへの着呼を検出し、利用者ＩＤおよびパスワードを認証サーバ中継機構１２に転送し、認証サーバ中継機構１２がテーブルを参照して当該利用者ＩＤのサービスの認証を担当するサーバに転送し、サーバが転送されてきた利用者ＩＤおよびパスワードをもとにテーブルを参照して当該利用者ＩＤおよびパスワードをチェックしてＯＫのときにサービスのアドレスを認証サーバ中継機構を介して分配機構４に通知し、分配機構４が指定されたアドレスに接続し、利用者端末１と該当するサービス１０を接続し、当該利用者端末１がサービス１０からサービス提供を受けるようにしている。

【００２４】この際、利用者ＩＤの一部をサービス１０に対応づけるようにしている。従って、同一公衆アクセスポイントから複数のサービス提供する際に、ネットワークでのユーザ認証を行なうと共に該当するサービス１０に分配して接続し、ネットワークの入口でセキュリティ管理を行うことにより、ネットワークセキュリティの信頼性を高めると共にサービス提供者のセキュリティ管理を高めたり、セキュリティ管理の負担を軽減したりすることが可能となる。

【００２５】

【発明の実施の形態】次に、図１から図３を用いて本発明の実施の形態および動作を順次詳細に説明する。ここ

で、図１の各機構を機能させるプログラムを図示外の記憶媒体から読み出して該当計算機システム（サーバなど）の主記憶上にローディングして起動し、以下に説明する各種処理を実行させるものである。

【００２６】図１は、本発明の１実施例構成図を示す。図１において、利用者端末１は、利用者が操作して利用者ＩＤおよびパスワードを入力してサービス１０に接続し、各種サービスの提供を受けるためのものである。

【００２７】公衆アクセスライン２は、ネットワーク３の任意のアクセスポイントに接続するものであって、例えば公衆回線である電話回線やＩＳＤＮ回線などである。利用者端末１は、この公衆アクセスライン２を用いてアクセスポイントＡＰの特定の電話番号に発呼し、サービス１０と接続して各種サービスの提供を受けるようにしている。

【００２８】ネットワーク３は、公衆アクセスラインの特定のアクセスポイントから接続する、サービス提供者側のネットワークであって、ここでは、分配機構４などを有するものである。

【００２９】分配機構４は、公衆アクセスラインからネットワーク３のアクセスポイントへの着信を受信したり、利用者端末１から受信した利用者ＩＤおよびパスワードをネットワーク認証機構６に転送したり、ネットワーク認証機構６から通知されたアドレスのサービス１０に、着呼した呼を接続したりなどするものである。

【００３０】サーバ５は、各種処理を行なうものであって、ここでは、ネットワーク認証機構６などから構成されるものである。ネットワーク認証機構６は、利用者ＩＤおよびパスワードをもとに認証を行なうものであって、ここでは、認証プログラム７、ユーザ情報テーブル８、および接続情報テーブル９などから構成されるものである。

【００３１】認証プログラム７は、利用者ＩＤおよびパスワードについて、ユーザ情報テーブル８を参照して認証を行い、ＯＫのときにサービス提供を行なうサービス１０のアドレスを接続情報テーブル９から取り出したりなどするものである。

【００３２】ユーザ情報テーブル８は、利用者ＩＤおよびパスワードを登録したものである。接続情報テーブル９は、利用者にサービスを提供するサービス１０のアドレスを登録したものである。

【００３３】次に、動作を説明する。図１において、　は、ユーザ認証要求（利用者ＩＤ／パスワード認証要求）を行なう。これは、分配機構４が利用者端末１から公衆アクセスライン２によってアクセスポイントＡＰに着呼したときに、送信されてきた利用者ＩＤおよびパスワードをサーバ５に転送する。

【００３４】　は、ユーザ認証回答（利用者ＩＤ／パスワードチェック回答、および接続ネットワークアドレス回答）を行なう。これは、　で転送を受けた利用者ＩＤおよびパスワードについて、サーバ５のネットワーク認証機構６を構成する認証プログラム７がユーザ情報テーブル８を参照して認証を行い（利用者ＩＤおよびパスワードが一致するかのチェックを行い）、ＯＫのときに接続情報テーブル９を参照して利用者ＩＤのプレフィックスに対応するネットワークアドレス（プレフィックスによって予め定められているサービス１０のアドレス）を取り出し、分配機構４に通知する。

【００３５】　は、ＩＤプレフィックスがＡの場合の接続である。これは、分配機構４が　で通知されたネットワークアドレスがＡの場合に、アクセスポイントに着呼した呼をネットワークアドレスＡのオンラインサービスＡに接続する。

【００３６】同様に、　、　は、ＩＤプレフィックスがＢあるいはＣの場合の接続である。これは、分配機構４が　で通知されたネットワークアドレスがＢあるいはＣの場合に、アクセスポイントに着呼した呼をネットワークアドレスＢのオンラインサービスＢに接続、あるいはネットワークアドレスＣのオンラインサービスＣに接続する。

【００３７】以上によって、利用者端末１から公衆アクセスラインを介してネットワークのアクセスポイントＡＰに着呼があったときに、送信されてきた利用者ＩＤおよびパスワードをネットワーク認証機構６に転送して認証を行い、ＯＫのときに通知された該当するオンラインサービスに接続し、サービスの提供を行なうことにより、ネットワークの入口で認証を行ってネットワークセキュリティを高信頼性にすることができると共に、ネットワーク認証を行った後に該当するサービス１０に振り分けて接続し、当該サービス１０で更に認証を行ってセキュリティを高めたり、あるいはネットワークの入口で既に認証がされているので当該サービス１０の入口で認証を省略したりすることが可能となる。

【００３８】図２は、本発明の他の実施例構成図を示す。ここで、利用者端末１、公衆アクセスライン２、ネットワーク３、およびサービス１０は、図１の同一番号のものと同じであるので説明を省略する。

【００３９】図２において、サーバ１１は、各種処理を行なうものであって、ここでは、認証サーバ中継機構１２などから構成されるものである。認証サーバ中継機構１２は、ネットワーク３の分配機構４から転送されてきた利用者ＩＤおよびパスワードを該当するネットワーク認証機構１６に転送したり、ネットワーク認証機構１６から通知された接続先のネットワークアドレスを分配機構４に通知したりなどするものであって、認証サーバ選択／中継プログラム１３およびサーバ対応テーブル１４などから構成されるものである。

【００４０】認証サーバ選択／中継プログラム１３は、サーバ対応テーブル１４を参照して利用者ＩＤのプレフィックスをもとに認証サーバを取り出し、利用者ＩＤお

よびパスワードをこのサーバに転送したり、認証結果を受け取ったときに分配機構４に通知したりなどするものである。

【００４１】サーバ対応テーブル１４は、利用者ＩＤのプレィックスに対応づけて認証を行なう認証サーバを予め登録したものである。サーバ１５は、利用者ＩＤおよびパスワードをもとに認証を行なうものであって、ここでは、ネットワーク認証機構１６などから構成されるものである。

【００４２】ネットワーク認証機構１６は、利用者ＩＤおよびパスワードをもとに認証を行なうものであって、ここでは、認証プログラム１７、ユーザ情報テーブル１８、およびアドレステーブル１９などから構成されるものである。このようにネットワーク認証機構１６をサービス１０毎に設けたことにより、サービス１０毎に一元的に利用者ＩＤおよびパスワードを管理し、図２に示す本願発明のネットワーク３の入口で認証を行なうルートと、図２以外の従来のサービス１０毎の専用のアクセスポイントへの利用者端末１からの利用者ＩＤおよびパスワードによる認証を並行して行なう場合に、サービス毎に一元的に利用者ＩＤおよびパスワードを容易に管理（利用者ＩＤおよびパスワードの新規登録、修正、削除など）することが可能となる。

【００４３】認証プログラム１７は、利用者ＩＤおよびパスワードについて、ユーザ情報テーブル１８を参照して認証を行い、ＯＫのときにサービス提供を行なうサービス１０のアドレスをアドレステーブル１９から取り出したりなどするものである。

【００４４】ユーザ情報テーブル１８は、利用者ＩＤおよびパスワードを登録したものである。アドレステーブル１９は、利用者にサービスを提供するサービス１０の接続ネットワークアドレスを登録したものである。

【００４５】次に、動作を説明する。図２において、　は、ユーザ認証要求（利用者ＩＤ／パスワード認証要求）を行なう。これは、分配機構４が利用者端末１から公衆アクセスライン２によってアクセスポイントＡＰに着呼したときに、送信されてきた利用者ＩＤおよびパスワードをサーバ１１転送する。

【００４６】　は、ＩＤプレフィックスにより認証サーバを選択し、ユーザ認証要求を中継する。これは、　で転送を受けた利用者ＩＤおよびパスワードについて、サーバ１１の認証サーバ中継機構１２を構成する認証サーバ選択／中継プログラム１３がサーバ対応テーブル１４を参照して利用者ＩＤのプレフィックスと一致する認証サーバを取り出し、ユーザ認証要求（利用者ＩＤ／パスワード認証要求）を中継する。

【００４７】　は、ユーザ認証回答（利用者ＩＤ／パスワードチェックおよび接続ネットワークアドレス回答）を行なう。これは、　で中継を受けた利用者ＩＤおよびパスワードについて、サーバ１５のネットワーク認証機構１６を構成する認証プログラム１７がユーザ情報テーブル１８を参照して認証を行い（利用者ＩＤおよびパスワードが一致するかのチェックを行い）、ＯＫのときにアドレステーブル１９を参照して接続ネットワークアドレスを取り出し、認証サーバ中継機構１２に通知する。

【００４８】　は、各サーバからのユーザ認証回答をアクセスポイントの分配機構４に中継する。これは、　で各サーバからのユーザ認証回答（ＯＫのときの接続ネットワークアドレスの回答）を分配機構４に通知する。

【００４９】　は、ＩＤプレフィックスがＡＡＡの場合の接続である。これは、分配機構４が　で通知された接続ネットワークアドレスがＡ．Ａ．Ａ．Ａ．の場合に、アクセスポイントに着呼した呼をネットワークアドレスＡ．Ａ．Ａ．Ａ．のオンラインサービスＡに接続する。

【００５０】同様に、　、　は、ＩＤプレフィックスがＢＢＢあるいはＣＣＣの場合の接続である。これは、分配機構４が　で通知された接続ネットワークアドレスがＢ．Ｂ．Ｂ．Ｂ．あるいは接続ネットワークアドレスがＣ．Ｃ．Ｃ．Ｃ．の場合に、アクセスポイントに着呼した呼をネットワークアドレスＢ．Ｂ．Ｂ．Ｂ．のオンラインサービスＢに接続、あるいはネットワークアドレスＣ．Ｃ．Ｃ．Ｃ．のオンラインサービスＣに接続する。

【００５１】以上によって、利用者端末１から公衆アクセスラインを介してネットワークのアクセスポイントＡＰに着呼があったときに、送信されてきた利用者ＩＤおよびパッスワードを認証サーバ中継機構１２に転送し、該当するネットワーク認証機構１６に中継して認証を行い、ＯＫのときに通知された該当するオンラインサービスに接続し、サービスの提供を行なうことにより、ネットワークの入口で認証を行ってネットワークセキュリティを高信頼性にすることができると共に、ネットワーク認証を行った後に該当するサービス１０に振り分けて接続し、当該サービス１０で更に認証を行ってセキュリティを高めたり、あるいはネットワークの入口で既に認証がされているので当該サービス１０の入口で認証を省略したりすることが可能となると共に、更に、サービス１０毎にネットワーク認証機構１６を設けて利用者ＩＤおよびパスワードの認証を行なことにより、サービス１０毎に一元的に管理（利用者ＩＤおよびパスワードの新規登録、修正、削除など）を行なうことが可能となる。

【００５２】次に、図３を用いて図２の構成の動作を詳細に説明する。図３は、本発明の動作説明図を示す。ここで、サーバＳは図２のサーバ１１を表し、サーバＳＡＡＡ、サーバＳＢＢＢ、サーバＳＣＣＣは図２のサーバ１５を表し、アクセスポイントは図２のアクセスポイントを表す。

【００５３】図３において、Ｓ１は、ＩＤ／ＰＷを受信する。これは、図２のサーバ１１の認証サーバ中継機構１２が利用者端末１からの利用者ＩＤおよびパスワードを受信する。

【００５４】Ｓ２は、先頭３文字を識別し、該当サーバにＩＤ／ＰＷを渡す。これは、Ｓ１で受信した利用者ＩＤの先頭３文字を識別、例えば利用者ＩＤのプレフィックスである先頭の３文字“ＡＡＡ”を識別し、図２のサーバ対応テーブル１４を参照して認証サーバ“ＳＡＡＡ”を取り出し、この認証サーバ“ＳＡＡＡ”に利用者ＩＤおよびパスワードを渡す。そして、この例では、Ｓ３ないしＳ９を行なう。

【００５５】Ｓ３は、オンラインサービスＡ用認証を行なう（ＩＤデータに対応する認証チェック）。これは、Ｓ２で利用者ＩＤプレフィックス＝ＡＡＡと判明し、利用者ＩＤおよびパスワードをサーバＳＡＡＡが渡されたので、図２の認証プログラム１７がユーザ情報テーブル１８を参照し、利用者ＩＤおよびパスワードが登録されているかチェックする。ＯＫの場合には、Ｓ４でネットワークアドレス（図２のアドレステーブル１９から取り出した接続ネットワークアドレス）をアクセスポイント（分配機構４）に返し、Ｓ６でオンラインサービスＡに呼を接続し、利用者端末１がオンラインサービスＡと接続してサービス提供を受ける。一方、ＮＧの場合には、Ｓ７で不可通知を返し、Ｓ８で受信した不可通知をアクセスポイントに返し、Ｓ９で分配機構４が呼を切断する。

【００５６】同様に、Ｓ２で利用者ＩＤプレフィックス＝ＢＢＢあるいは利用者ＩＤプレフィックス＝ＣＣＣと判明した場合、Ｓ１３ないしＳ１９、あるいはＳ２３ないしＳ２９によって認証ＯＫのときにオンラインサービスＢあるいはオンラインサービスＣに接続したり、一方、認証ＮＧのときに切断したりする。

【００５７】

【発明の効果】以上説明したように、本発明によれば、同一公衆アクセスポイントから複数のサービス提供する際に、ネットワークでのユーザ認証を行なうと共に該当するサービス１０に分配して接続し、ネットワークの入口でセキュリティ管理を行う構成を採用しているため、ネットワークセキュリティの信頼性を高めると共にサービス提供者のセキュリティ管理を高めたり、セキュリティ管理の負担を軽減したりすることができる。

【図面の簡単な説明】

【図１】本発明の１実施例構成図である。

【図２】本発明の他の実施例構成図である。

【図３】本発明の動作説明図である。

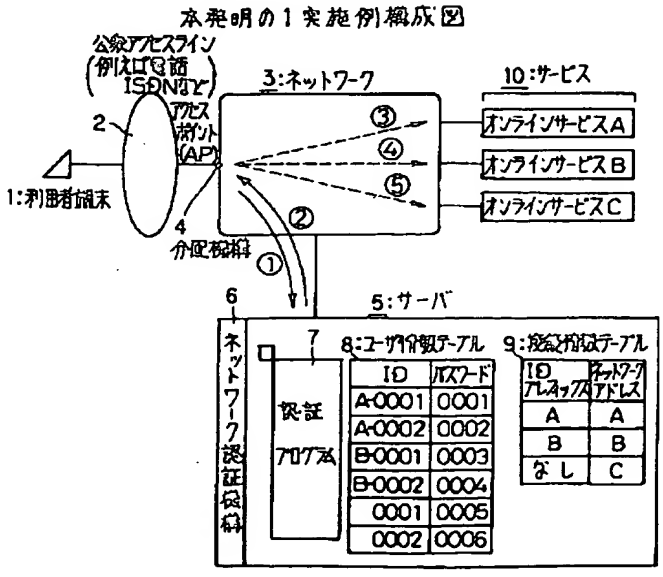
【図４】従来技術の説明図（その１）である。

【図５】従来技術の説明図（その２）である。

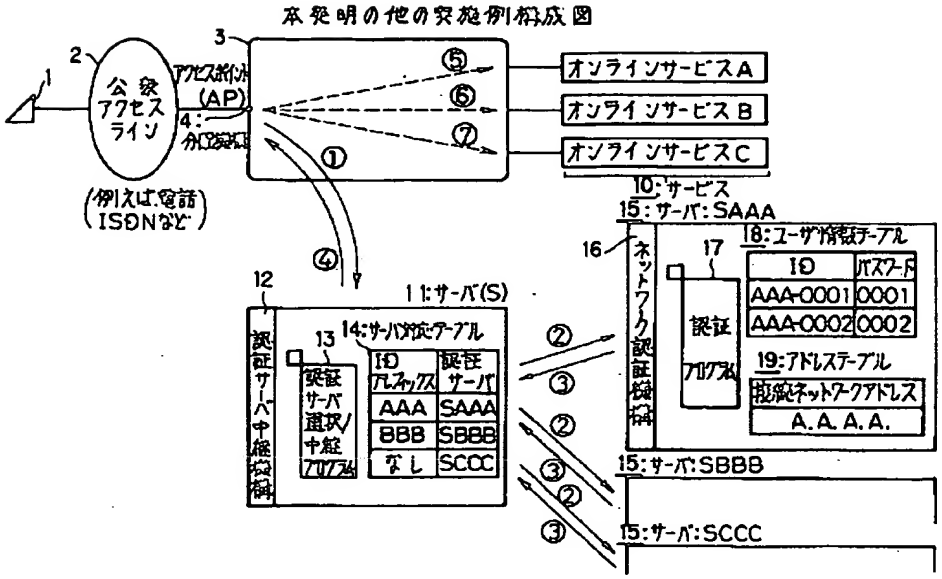
【符号の説明】

１：利用者端末
２：公衆アクセスライン（公衆回線網）
３：ネットワーク
４：分配機構
５、１１、１５：サーバ
６、１６：ネットワーク認証機構
７、１７：認証プログラム
８、１８：ユーザ情報テーブル
９：接続情報テーブル
１０：サービス
１２：認証サーバ中継機構
１３：認証サーバ選択／中継プログラム
１４：サーバ対応テーブル
１９：アドレステーブル

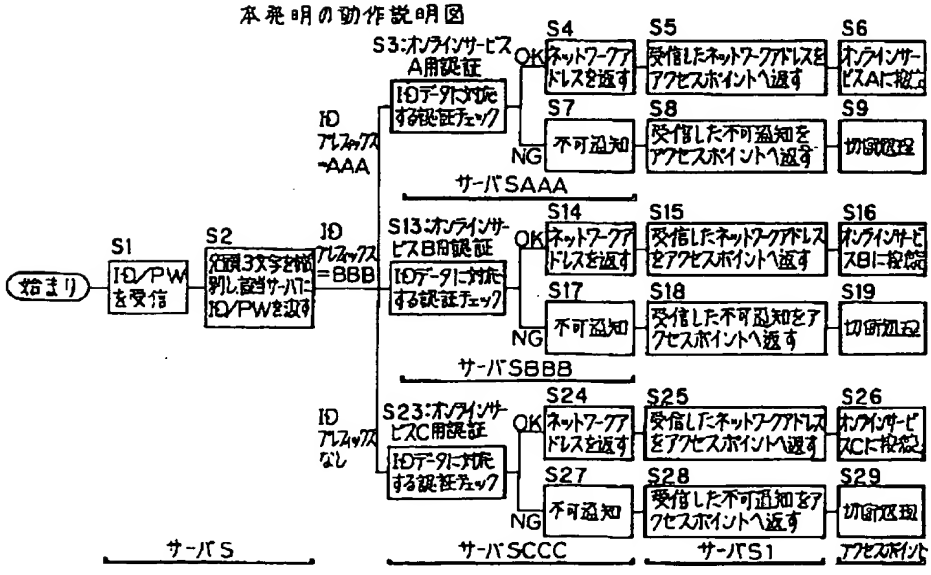
【図１】



【図２】

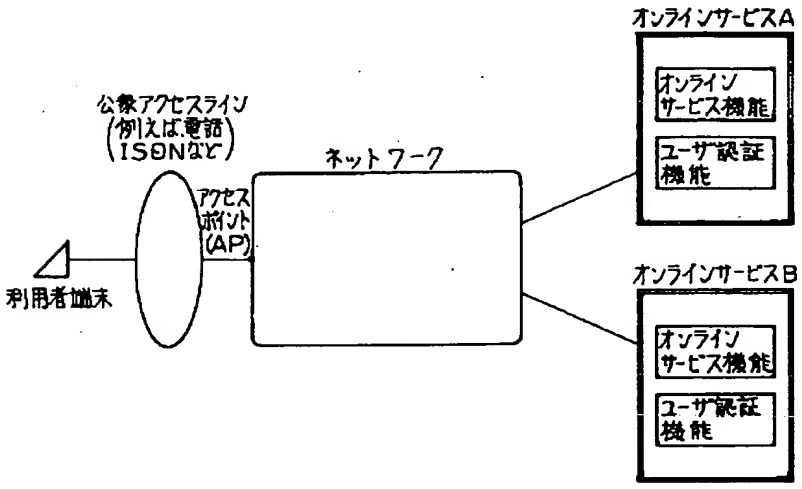

本発明の他の実施例構成図
公衆アクセスライン
(例えば電話ISDNなど)
アクセスポイント(AP)
オンラインサービスA
オンラインサービスB
オンラインサービスC
10:サービス
15:サーバ:SAAA
15:サーバ:SBBB
15:サーバ:SCCC
11:サーバ(S)
12
13
14:サーバ対応テーブル
16
17
18:ユーザ情報テーブル
19:アドレステーブル
ID
パスワード
AAA-0001
0001
AAA-0002
0002
AAA
SAAA
BBB
SBBB
なし
SCCC
A.A.A.A.

【図３】


本発明の動作説明図
始まり
S1
S2
S3:オンラインサービスA用認証
S4
S5
S6
S7
S8
S9
S13:オンラインサービスB用認証
S14
S15
S16
S17
S18
S19
S23:オンラインサービスC用認証
S24
S25
S26
S27
S28
S29
OK
NG
サーバS
サーバSCCC
サーバS1
アクセスポイント

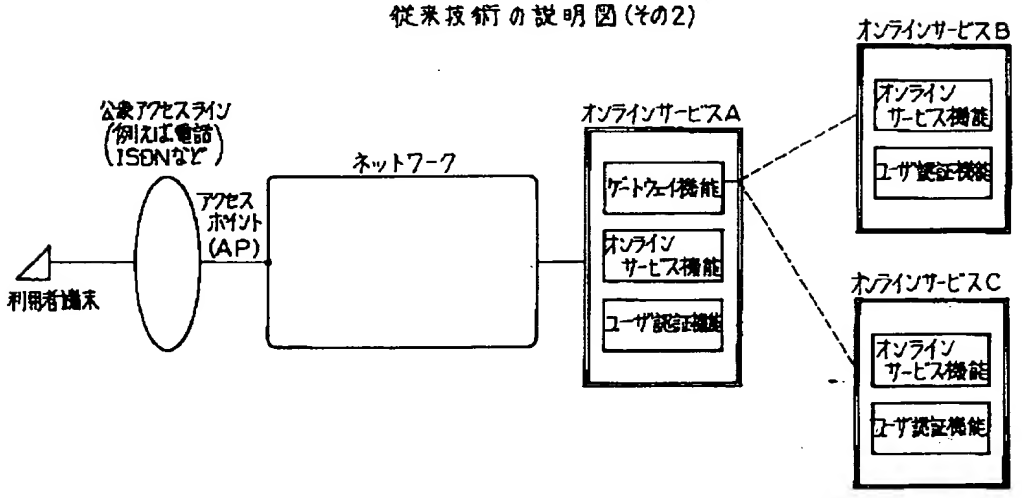
【図４】

従来技術の説明図(その1)



【図５】

従来技術の説明図(その2)



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI
H04M 11/00	302	H04L 11/26